

Security Agency, in coordination with the Director, shall perform a study on the use of active defense techniques to enhance the security of agencies, which shall include—

(1) a review of legal restrictions on the use of different active cyber defense techniques in Federal environments, in consultation with the Department of Justice;

(2) an evaluation of—

(A) the efficacy of a selection of active defense techniques determined by the Director of the Cybersecurity and Infrastructure Security Agency; and

(B) factors that impact the efficacy of the active defense techniques evaluated under subparagraph (A);

(3) recommendations on safeguards and procedures that shall be established to require that active defense techniques are adequately coordinated to ensure that active defense techniques do not impede threat response efforts, criminal investigations, and national security activities, including intelligence collection; and

(4) the development of a framework for the use of different active defense techniques by agencies.

#### **SEC. 5182. SECURITY OPERATIONS CENTER AS A SERVICE PILOT.**

(a) **PURPOSE.**—The purpose of this section is for the Cybersecurity and Infrastructure Security Agency to run a security operation center on behalf of another agency, alleviating the need to duplicate this function at every agency, and empowering a greater centralized cybersecurity capability.

(b) **PLAN.**—Not later than 1 year after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall develop a plan to establish a centralized Federal security operations center shared service offering within the Cybersecurity and Infrastructure Security Agency.

(c) **CONTENTS.**—The plan required under subsection (b) shall include considerations for—

(1) collecting, organizing, and analyzing agency information system data in real time;

(2) staffing and resources; and

(3) appropriate interagency agreements, concepts of operations, and governance plans.

(d) **PILOT PROGRAM.**—

(1) **IN GENERAL.**—Not later than 180 days after the date on which the plan required under subsection (b) is developed, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director, shall enter into a 1-year agreement with not less than 2 agencies to offer a security operations center as a shared service.

(2) **ADDITIONAL AGREEMENTS.**—After the date on which the briefing required under subsection (e)(1) is provided, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director, may enter into additional 1-year agreements described in paragraph (1) with agencies.

(e) **BRIEFING AND REPORT.**—

(1) **BRIEFING.**—Not later than 260 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Oversight and Reform of the House of Representatives a briefing on the parameters of any 1-year agreements entered into under subsection (d)(1).

(2) **REPORT.**—Not later than 90 days after the date on which the first 1-year agreement entered into under subsection (d) expires, the Director of the Cybersecurity and Infrastructure Security Agency shall submit to the

Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Oversight and Reform of the House of Representatives a report on—

(A) the agreement; and

(B) any additional agreements entered into with agencies under subsection (d).

**SA 4675.** Mr. SULLIVAN submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle E of title VIII, add the following:

#### **SEC. 857. PROHIBITION ON CONTRACTS THAT BENEFIT CHINESE COMMUNIST PARTY.**

(a) **IN GENERAL.**—The Secretary of Defense may not enter into a contract for defense articles or services that are—

(1) developed or manufactured by, or include parts from, the Chinese Communist Party;

(2) provided by an entity that has suspected ties to the Chinese Communist Party; or

(3) provided by an entity that provides defense articles or services, including research, engineering, and technology, to the Chinese Communist Party.

(b) **DEFENSE ARTICLES OR SERVICES DEFINED.**—In this section, the term “defense articles or services” means defense articles or services designated by the President under section 38(a)(1) of the Arms Export Control Act (22 U.S.C. 2778(a)(1)).

**SA 4676.** Ms. KLOBUCHAR submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place in title X, insert the following:

#### **SEC. \_\_\_\_ . VETERANS CYBERSECURITY AND DIGITAL LITERACY GRANT PROGRAM.**

(a) **FINDINGS.**—Congress finds the following:

(1) Adversaries from Russia, China, and Iran are using information warfare to influence democracies across the world, and extremist organizations often use digital communications to recruit members. Influence campaigns from foreign adversaries reached tens of millions of voters during the 2016 and 2018 elections with racially and divisively targeted messages. The United States can fight these influences by ensuring that citizens of the United States possess the necessary skills to discern disinformation and misinformation and protect themselves from foreign influence campaigns.

(2) Researchers have documented persistent, pervasive, and coordinated online targeting of members of the Armed Forces, veterans, and their families by foreign adver-

saries seeking to undermine United States democracy in part because of public trust placed in these communities.

(3) A 2017 report by the University of Oxford's Graphika Institute, titled “Social Media Disinformation Campaigns Against US Military Personnel and Veterans”, concluded that “The public tends to place trust in military personnel and veterans, making them potentially influential voters and community leaders. Given this trust and their role in ensuring national security, these individuals have the potential to become particular targets for influence operations and information campaigns conducted on social media. There are already reports of US service personnel being confronted by foreign intelligence agencies while posted abroad, with details of their personal lives gleaned from social media.”.

(4) The Select Committee on Intelligence of the Senate found in its investigation of the interference in the 2016 election that social media posts by the Internet Research Agency (IRA) of Russia reached tens of millions of voters in 2016 and were meant to pit the people of the United States against one another and sow discord. Volume II of the Committee's investigation found that the Internet Research Agency's Instagram account with the second largest reach used the handle “@american.veterans” and was “aimed at patriotic, conservative audiences, collected 215,680 followers, and generated nearly 18.5 million engagements.”.

(5) A 2019 investigative report by the Vietnam Veterans of America (VVA) titled “An Investigation into Foreign Entities who are Targeting Troops and Veterans Online”, found that the Internet Research Agency targeted veterans and the followers of several congressionally chartered veterans service organizations with at least 113 advertisements during and following the 2016 election and that “this represents a fraction of the Russian activity that targeted this community with divisive propaganda.”. The report also found that foreign actors have been impersonating veterans through social-media accounts and interacting with veterans and veterans groups on social media to spread propaganda and disinformation. To counter these acts, Vietnam Veterans of America recommended that the Department of Veterans Affairs “immediately develop plans to make the cyber-hygiene of veterans an urgent priority within the Department of Veterans Affairs. The VA must educate and train veterans on personal cybersecurity: how to mitigate vulnerabilities, vigilantly maintain safe practices, and recognize threats, including how to identify instances of online manipulation.”.

(6) The Cyberspace Solarium Commission, a bicameral and bipartisan commission, established by section 1652 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232), concluded in its finished report that the “U.S. government should promote digital literacy, civics education, and public awareness to build societal resilience to foreign, malign cyber-enabled information operations and that the U.S. government must ensure that individual Americans have both the digital literacy tools and the civics education they need to secure their networks and their democracy from cyber-enabled information operations.”. The report recommended that Congress authorizing grant programs to do this.

(b) **SENSE OF CONGRESS.**—It is the sense of Congress that, given the threat foreign influence campaigns pose for United States democracy and the findings and recommendations of Congress and experts, Congress must immediately act to pass legislative measures

to increase digital and media literacy as well as cyber-hygiene among veterans.

(c) **PROGRAM REQUIRED.**—The Secretary shall establish a program to promote digital citizenship and media literacy, through which the Secretary shall award grants to eligible entities to enable those eligible entities to carry out the activities described in subsection (e).

(d) **APPLICATION.**—An eligible entity seeking a grant under the program required by subsection (c) shall submit to the Secretary an application therefor at such time, in such manner, and containing such information as the Secretary may require, including, at a minimum the following:

(1) A description of the activities the eligible entity intends to carry out with the grant funds.

(2) An estimate of the costs associated with such activities.

(3) Such other information and assurances as the Secretary may require.

(e) **ACTIVITIES.**—An eligible entity shall use the amount of a grant awarded under the program required by subsection (c) to carry out one or more of the following activities to improve cyber-hygiene and increase digital and media literacy among veterans:

(1) Develop competencies in cyber-hygiene.

(2) Develop media literacy and digital citizenship competencies by promoting veterans'—

(A) research and information fluency;

(B) critical thinking and problem solving skills;

(C) technology operations and concepts;

(D) information and technological literacy;

(E) concepts of media and digital representation and stereotyping;

(F) understanding of explicit and implicit media and digital messages;

(G) understanding of values and points of view that are included and excluded in media and digital content;

(H) understanding of how media and digital content may influence ideas and behaviors;

(I) understanding of the importance of obtaining information from multiple media sources and evaluating sources for quality;

(J) understanding how information on digital platforms can be altered through algorithms, editing, and augmented reality;

(K) ability to create media and digital content in civically and socially responsible ways; and

(L) understanding of influence campaigns conducted by foreign adversaries and the tactics employed by foreign adversaries for conducting influence campaigns.

(f) **REPORTING.**—

(1) **REPORTS BY GRANT RECIPIENTS.**—Each recipient of a grant under the program required by subsection (c) shall, not later than one year after the date on which the recipient first receives funds pursuant to the grant, submit to the Secretary a report describing the activities the recipient carried out using grant funds and the effectiveness of those activities.

(2) **REPORT BY THE SECRETARY.**—Not later than 90 days after the date on which the Secretary receives the last report the Secretary expects to receive under paragraph (1), the Secretary shall submit to Congress a report describing the activities carried out under this section and the effectiveness of those activities.

(g) **SENSE OF CONGRESS.**—It is the sense of Congress that the Secretary should—

(1) establish and maintain a list of eligible entities that receive a grant under the program required by subsection (c), and individuals designated by those eligible entities as participating individuals; and

(2) make that list available to those eligible entities and participating individuals in order to promote communication and further

exchange of information regarding sound digital citizenship and media literacy practices among recipients of grants under the program required by subsection (c).

(h) **AUTHORIZATION OF APPROPRIATIONS.**—There is authorized to be appropriated to carry out this section \$20,000,000 for fiscal year 2022.

(i) **DEFINITIONS.**—In this section:

(1) **CYBER-HYGIENE.**—The term “cyber-hygiene” means practices and steps that users of computers and other internet connected devices take to maintain and improve online security, maintain the proper functioning of computers devices, and protect computers and devices from cyberattacks and unauthorized use.

(2) **DIGITAL CITIZENSHIP.**—The term “digital citizenship” means the ability to—

(A) safely, responsibly, and ethically use communication technologies and digital information technology tools and platforms;

(B) create and share media content using principles of social and civic responsibility and with awareness of the legal and ethical issues involved; and

(C) participate in the political, economic, social, and cultural aspects of life related to technology, communications, and the digital world by consuming and creating digital content, including media.

(3) **ELIGIBLE ENTITY.**—The term “eligible entity” means—

(A) a civil society organization, including community groups, nongovernmental organizations, nonprofit organization, labor organizations, indigenous groups, charitable organizations, professional associations, and foundations; and

(B) congressionally chartered veterans service organizations.

(4) **MEDIA LITERACY.**—The term “media literacy” means the ability to—

(A) access relevant and accurate information through media in a variety of forms;

(B) critically analyze media content and the influences of different forms of media;

(C) evaluate the comprehensiveness, relevance, credibility, authority, and accuracy of information;

(D) make educated decisions based on information obtained from media and digital sources;

(E) operate various forms of technology and digital tools; and

(F) reflect on how the use of media and technology may affect private and public life.

(5) **SECRETARY.**—The term “Secretary” means the Secretary of Veterans Affairs.

**SA 4677.** Ms. KLOBUCHAR submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle A of title XII, add the following:

**SEC. 1210. GLOBAL ELECTORAL EXCHANGE PROGRAM.**

(a) **SHORT TITLE.**—This section may be cited as the “Global Electoral Exchange Act of 2021”.

(b) **SENSE OF CONGRESS.**—It is the sense of Congress that—

(1) recent elections globally have illustrated the urgent need for the promotion and exchange of international best election prac-

tices, particularly in the areas of cybersecurity, results transmission, transparency of electoral data, election dispute resolution, and the elimination of discriminatory registration practices and other electoral irregularities;

(2) the advancement of democracy worldwide promotes United States interests, as stable democracies provide new market opportunities, improve global health outcomes, and promote economic freedom and regional security;

(3) credible elections are the cornerstone of a healthy democracy and enable all persons to exercise their basic human right to have a say in how they are governed;

(4) inclusive elections strengthen the credibility and stability of democracies more broadly;

(5) at the heart of a strong election cycle is the professionalism of the election management body and an empowered civil society;

(6) the development of local expertise via peer-to-peer learning and exchanges promotes the independence of such bodies from internal and external influence; and

(7) supporting the efforts of peoples in democratizing societies to build more representative governments in their respective countries is in the national interest of the United States.

(c) **GLOBAL ELECTORAL EXCHANGE.**—

(1) **IN GENERAL.**—The Global Engagement Center (referred to in this section as the “Center”) at the Department of State is authorized to establish and administer a Global Electoral Exchange Program (referred to in this section as the “Program”) to promote the utilization of sound election administration practices around the world.

(2) **PURPOSE.**—The purpose of the Program shall include the promotion and exchange of international best election practices, including in the areas of—

(A) cybersecurity;

(B) the protection of election systems against influence campaigns;

(C) results transmission;

(D) transparency of electoral data;

(E) election dispute resolution;

(F) the elimination of discriminatory registration practices and electoral irregularities;

(G) inclusive and equitable promotion of candidate participation;

(H) equitable access to polling places, voter education information, and voting mechanisms (including by persons with disabilities); and

(I) other sound election administration practices.

(3) **EXCHANGE OF ELECTORAL AUTHORITIES.**—

(A) **IN GENERAL.**—The Center, in consultation, as appropriate, with the United States Agency for International Development, may award grants to any United States-based organization that—

(i) is described in section 501(c)(3) of the Internal Revenue Code of 1986 and exempt from tax under section 501(a) of such Code;

(ii) has experience in, and a primary focus on, foreign comparative election systems or subject matter expertise in the administration or integrity of such systems; and

(iii) submits an application in such form, and satisfying such requirements, as the Center may require.

(B) **TYPES OF GRANTS.**—An organization described in subparagraph (A) may receive a grant under this paragraph to design and implement programs that—

(i) bring to the United States election administrators and officials, including government officials, poll workers, civil society representatives, members of the judiciary, and others who participate in the organization and administration of public elections in a foreign country that faces challenges to